АЛГЕБРА 1

Групе

Групе малог реда; класе конјугације

Зоран Петровић

23. новембар 2011.

Како израчунати $\varphi(n)$ за произвољно $n \geq 2$? За функцију φ важи следеће:

1. уколико су m и n узајамно прости, онда је $\varphi(mn) = \varphi(m)\varphi(n)$;
2. за сваки прост број p и $m \geq 1$: $\varphi(p^m) = p^m - p^{m-1}$.

Прву особину доказаћемо када се будемо бавили комутативним прстенима са јединицом, док се друга лако доказује. Наиме, $x \in Z_{p^m} \setminus \{0\}$ није у $\Phi(p^m)$ ако и само ако $p \mid x$. Дакле, $x \in \{p, 2p, \ldots, (p^{m-1}-1)p\}$. Према томе,

$$\varphi(p^m) = |\Phi(p^m)| = (p^m - 1) - (p^{m-1} - 1) = p^m - p^{m-1}.$$

Коришћењем ова два својства, добијамо да важи следећи резултат. Ако је $n = p_1^{m_1} p_2^{m_2} \cdots p_k^{m_k}$ факторизација броја n на просте факторе, онда је

$$\begin{aligned}
\varphi(n) &= \varphi(p_1^{m_1} p_2^{m_2} \cdots p_k^{m_k}) \\
&= \varphi(p_1^{m_1})\varphi(p_2^{m_2}) \cdots \varphi(p_k^{m_k}) \\
&= p_1^{m_1-1}(p_1-1)p_2^{m_2-1}(p_2-1)\cdots p_k^{m_k-1}(p_k-1) \\
&= p_1^{m_1}\left(1-\frac{1}{p_1}\right)p_2^{m_2}\left(1-\frac{1}{p_2}\right)\cdots p_k^{m_k}\left(1-\frac{1}{p_k}\right) \\
&= n\left(1-\frac{1}{p_1}\right)\left(1-\frac{1}{p_2}\right)\cdots\left(1-\frac{1}{p_k}\right).
\end{aligned}$$

Лагранжова теорема нам показује да нпр. група реда 20 не може да има подгрупу реда 12 и сл. Она нам не говори ништа о томе да ли нпр. група реда 20 има подгрупу реда 10 (постојање такве подгрупе не би било у супротности са Лагранжовом теоремом). Оваква питања су знатно сложенија и ми се њима нећемо много бавити. Само ћемо навести једну теорему, која говори о постојању подгрупа одређеног реда и навести неке њене последице у облику примера.

Теорема 1 (Кошијева теорема) Ако је G коначна група и p прост број такав да $p \mid |G|$, онда у G постоји елемент реда p.

Дакле, уколико је p прост број, који дели ред групе G, у G постоји елемент реда p, а самим тим и подгрупа реда p.

Пример 2 Свака група реда 6 изоморфна је или групи $\mathbb{Z}_6$ или групи $\mathbb{D}_3$.

Нека је $|G| = 6$. Уколико у G постоји елемент реда 6, онда је $G \cong \mathbb{Z}_6$. Претпоставимо стога да у G не постоји елемент реда 6. На основу Кошијеве теореме у G постоји елемент x реда 3 и елемент y реда 2. Како је $\omega(x) = \omega(x^2)$, то $y \notin \langle x \rangle$. Стога је

$$G = \langle x \rangle \sqcup y\langle x \rangle = \{e, x, x^2, y, yx, yx^2\}.$$

Елемент xy је у G и једнак је неком од наведених елемената. Није тешко уверити се (уверите се!) да су једине могућности:

1. $xy = yx$;
2. $xy = yx^2$.

Но, ако је $xy = yx$, добијамо да је

$$G \cong \langle y \rangle \times \langle x \rangle \cong \mathbb{Z}_6$$

(зашто?), што противречи претпоставци да у G нема елемената реда 6. Преостаје могућност $xy = yx^2$ и у том случају је $G \cong \mathbb{D}_3$ (при изоморфизму који x слика у ρ, а y у σ). ♣

Завршићемо ову лекцију описом група реда 8. Да бисмо могли да је извршимо, биће нам потребан још један пример групе.

Добро нам је познато рачунање са комплексним бројевима. Сваки комплексан број се може написати у облику $a + bi$, где су a и b реални бројеви, а i је имагинарна јединица, тј. за i важи следеће: $i^2 = -1$. Хамилтон је у математику увео кватернионе. Сваки кватернион може се написати у облику $a + bi + cj + dk$, где су a, b, c, d реални бројеви, а i, j, k имагинарне јединице за које још важи: $ij = k = -ji, jk = i = -kj, ki = j = -ik$. Као што се може видети, множење кватерниона није комутативно, но многа друга својства, која важе за комплексне бројеве важе и за кватернионе. Наравно, и поред занимљивости овог појма, ми се нећемо њима детаљно бавити. Но, означимо са Q_8 следећи скуп:

$$Q_8 = \{1, -1, i, -i, j, -j, k, -k\}.$$

Није тешко уверити се да је $(Q_8, \cdot)$ група. Зовемо је кватернионска група.

Наведимо таблицу ове групе.

$\cdot$	1	-1	i	$-i$	j	$-j$	k	$-k$
1	1	-1	i	$-i$	j	$-j$	k	$-k$
-1	-1	1	$-i$	i	$-j$	j	$-k$	k
i	i	$-i$	-1	1	k	$-k$	$-j$	j
$-i$	$-i$	i	1	-1	$-k$	k	j	$-j$
j	j	$-j$	$-k$	k	-1	1	i	$-i$
$-j$	$-j$	j	k	$-k$	1	-1	$-i$	i
k	k	$-k$	j	$-j$	$-i$	i	-1	1
$-k$	$-k$	k	$-j$	j	i	$-i$	1	-1

Приметимо да је Q_8 генерисана елементима i и j и да за ове елементе важи: $i^2 = j^2$ и $jij^{-1} = i^{-1}$.

Пример 3 Свака група реда 8 изоморфна је тачно једној од група:

$$\mathbb{Z}_8, \quad \mathbb{Z}_2 \times \mathbb{Z}_4, \quad \mathbb{Z}_2 \times \mathbb{Z}_2 \times \mathbb{Z}_2, \quad \mathbb{D}_4, \quad Q_8.$$

Нека је G група реда 8. Уколико у G постоји елемент реда 8, онда је $G \cong \mathbb{Z}_8$. Уколико је пак у G сваки елемент реда 2, према ранијем резултату следи да је $G \cong \mathbb{Z}_2 \times \mathbb{Z}_2 \times \mathbb{Z}_2$. Претпоставимо у даљем да у G постоји елемент реда 4 и да не постоји елемент реда 8.

Нека је x реда 4 и нека $y \notin \langle x \rangle$. Тада је

$$G = \langle x \rangle \sqcup y\langle x \rangle = \{e, x, x^2, x^3, y, yx, yx^2, yx^3\}.$$

Одредимо који од ових елемената може бити једнак елементу xy. Пре свега, како $y \notin \langle x \rangle$ и како је $x \neq e$, то $xy \notin \{e, x, x^2, x^3, y\}$. Уколико је пак $xy = yx^2$, добијамо да је $x = yx^2y^{-1}$ из чега следи да је $x^2 = yx^4y^{-1} = yey^{-1} = e$, па би x био реда 2, што није. Закључујемо да $xy \in \{yx, yx^3\}$.

Одредимо још колико је y^2. Пре свега, како $y \notin \langle x \rangle$, то $y^2 \notin y\langle x \rangle$. Осим тога, како је $\omega(x) = \omega(x^3) = 4$, а у G нема елемената реда 8 то y^2 не може бити ни x ни x^3. Дакле, $y^2 \in \{e, x^2\}$.

Добили смо 4 случаја

1. $xy = yx$, $y^2 = e$;
2. $xy = yx$, $y^2 = x^2$;
3. $xy = yx^3$, $y^2 = e$;
4. $xy = yx^3$, $y^2 = x^2$.

Размотримо сваки посебно.

1. У овом случају је група G комутативна и функција $f\colon \mathbb{Z}_2 \times \mathbb{Z}_4 \to G$ дефинисана са $f(r, s) = y^r x^s$ је изоморфизам. Јасно је да је f бијекција. Само треба проверити слагање са операцијама.

$$f(r +_2 r', s +_4 s') = y^{r+_2 r'} x^{s+_4 s'}.$$

Како је y реда 2 и x реда 4, то је $y^{r+_2 r'} = y^r y^{r'}$ и $x^{s+_4 s'} = x^s x^{s'}$. Дакле,

$$f(r +_2 r', s +_4 s') = y^r y^{r'} x^s x^{s'}.$$

Како је $xy = yx$, то је

$$y^r y^{r'} x^s x^{s'} = y^r x^s y^{r'} x^{s'} = f(r,s) f(r',s').$$

Дакле, заиста је

$$f(r +_2 r', s +_4 s') = f(r,s) f(r',s').$$

2. У овом случају је такође група G комутативна. Приметимо да је сада елемент y реда 4, но елемент $y^3 x$ је реда 2:

$$(y^3 x)^2 = y^6 x^2 = x^6 x^2 = x^8 = e.$$

Стога је изоморфизам $f\colon \mathbb{Z}_2 \times \mathbb{Z}_4 \to G$ задат са: $f(r,s) = (y^3 x)^r x^s$. Проверите детаље!

3. У овом случају, ситуација је јасна. Изоморфизам $f\colon \mathbb{D}_4 \to G$ задат је са: $f(\sigma) = y$, $f(\rho) = x$.

4. И у овом случају није тешко видети како функција $f\colon Q_8 \to G$ задата са: $f(i) = x$, $f(j) = y$ задаје изоморфизам (важно је приметити да је $ij = k = ji^3$ и $i^2 = j^2$). ♣

Уведимо сада један веома важан појам.

Дефиниција 4 Елемент y је конјугован елементу x (елемент y је конјугат елемента x) у групи G уколико постоји $g \in G$ тако да је

$$y = gxg^{-1}.$$

Јасно је да је на овај начин дефинисана једна релација еквиваленције на скупу G. Наиме, сваки елемент x је конјугован сам себи пошто је $x = exe^{-1}$. Уколико је y конјугован елементу x, тј. постоји $g \in G$ тако да је $y = gxg^{-1}$, онда је и x конјугован y, јер је $x = g^{-1} y (g^{-1})^{-1}$. Ако је y конјугован елементу x ($y = gxg^{-1}$ за неко $g \in G$), а z конјугован елементу y ($z = hyh^{-1}$), онда је и z конјугован елементу x: $z = (hg)x(hg)^{-1}$.

Класу еквиваленције при овој релацији зовемо класа конјугације (или класа конјугованости).

Пример 5 Одредити класе конјугације у групи $\mathbb{D}_n$.

Разликоваћемо два случаја.

1. $\underline{n = 2l+1}$: Из

$$(\sigma\rho^s)\sigma(\sigma\rho^s)^{-1} = \sigma\rho^s\sigma\sigma\rho^s = \sigma\rho^{2s}$$

и

$$\rho^s\sigma\rho^{-s} = \sigma\rho^{-2s} = \sigma\rho^{2l+1-2s}$$

следи да је једна класа конјугације

$$\{\sigma, \sigma\rho, \sigma\rho^2, \ldots, \sigma\rho^{2l}\}.$$

Из

$$(\sigma\rho^s)\rho^k(\sigma\rho^s)^{-1} = \sigma\rho^s\rho^k\sigma\rho^s = \sigma\sigma\rho^{-s}\rho^{-k}\rho^s = \rho^{-k} = \rho^{2l+1-k},$$

као и из чињенице да је $\rho^s\rho^k\rho^{-s} = \rho^k$, следи да су

$$\{\rho, \rho^{2l}\}, \quad \{\rho^2, \rho^{2l-1}\}, \quad \ldots \quad , \{\rho^l, \rho^{l+1}\}$$

такође класе конјугације. Осим тога, $\{\varepsilon\}$ је једина преостала класа конјугације.

2. $\underline{n = 2l}$: Како је

$$(\sigma\rho^s)\sigma(\sigma\rho^s)^{-1} = \sigma\rho^{2s} \quad \text{и} \quad (\sigma\rho^s)\sigma\rho(\sigma\rho^s)^{-1} = \sigma\rho^{2s-1},$$

а

$$\rho^s\sigma\rho^{-s} = \sigma\rho^{-2s} = \sigma\rho^{2l-2s} \quad \text{и} \quad \rho^s\sigma\rho\rho^{-s} = \sigma\rho^{1-2s} = \sigma\rho^{2l+1-2s}$$

то је класа конјугације елемента σ једнака $\{\sigma\rho^{2s} : 0 \leq s \leq l-1\}$, а класа конјугације елемента $\sigma\rho$ је $\{\sigma\rho^{2s+1} : 0 \leq s \leq l-1\}$. Осим тога, како је $\rho^s\rho^k\rho^{-s} = \rho^k$, а

$$(\sigma\rho^s)\rho^k(\sigma\rho^s)^{-1} = \sigma\rho^s\rho^k\sigma\rho^s = \rho^{-k} = \rho^{2l-k},$$

то су двочлане класе конјугације:

$$\{\rho, \rho^{2l-1}\}, \{\rho^2, \rho^{2l-2}\}, \quad \ldots \quad , \{\rho^{l-1}, \rho^{l+1}\},$$

док се једине преостале класе конјугације једночлане:

$$\{\varepsilon\}, \quad \{\rho^l\}.$$

Приметимо на крају да у случају да је n непарно у $\mathbb{D}_n$ постоји само једна једночлана класа конјугације, док их у случају да је n парно има две. ♣

Пример 6 Испитајмо како изгледају класе конјугације у групи S_n и одредимо их за групе S_4 и A_4.

Приметимо најпре да су ма која два цикла исте дужине конјугована. Наиме, ако су $(a_1a_2\ldots a_k)$ и $(b_1b_2\ldots b_k)$ цикли дужине k $\underline{\text{из}}$ S_n и ако је π нека пермутација из S_n за коју је $\pi(a_i) = b_i$ за све $i = \overline{1,k}$, тада је

$$\pi(a_1a_2\ldots a_k)\pi^{-1} = (\pi(a_1)\pi(a_2)\ldots\pi(a_k)) = (b_1b_2\ldots b_k).$$

Општије, важи следеће. Две пермутације σ и ρ из S_n су конјуговане ако и само ако имају исту циклусну структуру, тј. ако у растављању на производ дисјунктних циклуса у пермутацији σ има исти број циклуса дужине $1, 2, 3, \ldots$ као и у пермутацији ρ. Ово није тешко доказати, али због уштеде времена, доказ нећемо исписивати. Но, резултат би требало да буде очигледан из претходно наведене једнакости.

Позабавимо се сада класама конјугације у групама S_4 и A_4.

У случају групе S_4, можемо користити наведени резултат. Добијамо да су класе конјугације следеће:

$$\{(1234), (1324), (2134), (2314), (3124), (3214)\};$$

$$\{(123), (132), (124), (142), (134), (143), (234), (243)\};$$

$$\{(12), (13), (14), (23), (24), (34)\};$$

$$\{(12)(34), (13)(24), (14)(23)\};$$

$$\{(1)\}.$$

Видимо да постоји само једна једночлана класа конјугације.

У случају групе A_4 морамо пажљивије радити. Нпр. у A_4 циклуси (123) и (132) нису конјуговани. Наиме, ако је π пермутација за коју је

$$\pi(123)\pi^{-1} = (132),$$

она *није* парна пермутација. Наиме, $\pi(4) = 4$, а осим тога мора бити $(\pi(1)\pi(2)\pi(3)) = (132)$, што оставља следеће могућности за π: $\pi = (23)$, или $\pi = (12)$, или $\pi = (23)$. Ниједна од ових пермутација није парна. Дакле, елементи (123) и (132) нису у истој класи конјугације у A_4. Но, ипак није тешко уверити се да су класе конјугације дате са:

$$\{(123), (124), (134), (234)\};$$

$$\{(132), (142), (143), (243)\};$$

$$\{(12)(34), (13)(24), (14)(23)\};$$

$$\{(1)\}.$$

Видимо да и у овом случају постоји само једна једночлана класа конјугације. □

Дефиниција 7 Нека је G група. Центар групе G, у ознаци $Z(G)$ дефинише се као скуп свих елемената из G, који комутирају са свим елементима те групе:

$$Z(G) := \{x \in G : (\forall g \in G) gx = xg\}.$$

Није тешко проверити да је $Z(G)$ једна подгрупа групе G. Наиме, како је $eg = ge$ за све $g \in G$, то $e \in Z(G)$. Ако $x, y \in Z(G)$, онда

$$(xy)g = x(yg) = x(gy) = (xg)y = (gx)y = g(xy),$$

па $xy \in Z(G)$. Осим тога, ако је $x \in Z(G)$, тј. за све $g \in G$ важи $xg = gx$, онда, множећи ову једнакост здесна и слева са x^{-1}, добијамо $gx^{-1} = x^{-1}g$. Закључујемо да и x^{-1} припада центру.

Веза између центра и конјугације дата је следећим ставом чији доказ следи непосредно из дефиниције центра.

Став 8 Центар групе G је унија свих једночланих класа конјугације.

Пример 9 Центар групе $\mathbb{D}_n$ је тривијалан уколико је n непаран број, а једнак је $\{\varepsilon, \rho^{n/2}\}$ уколико је n паран број.

Претпоставимо да је елемент $\sigma\rho^k$ у центру групе $\mathbb{D}_n$. То значи да је

$$(\sigma\rho^k)\rho = \rho(\sigma\rho^k),$$

тј.

$$\sigma\rho^{k+1} = \sigma\rho^{k-1}.$$

Одавде следи да је $\rho^2 = \varepsilon$, што није могуће. Дакле, можемо да закључимо да ниједан елемент облика $\sigma\rho^k$ не може бити у $Z(\mathbb{D}_n)$.

Посматрајмо елементе облика ρ^k за $1 \leq k < n$. Уколико је неки такав елемент у центру, мора бити

$$\rho^k(\sigma\rho) = (\sigma\rho)\rho^k,$$

па је

$$\sigma\rho^{-k}\rho = \sigma\rho^{k+1}.$$

Добијамо да мора бити $\rho^{2k} = \varepsilon$. Како је $n = \omega(\rho)$, добијамо да $n \mid 2k$. Уколико је n непаран, добили бисмо да $n \mid k$, што није могуће ($1 \leq k < n$). Дакле, центар групе $\mathbb{D}_n$ је тривијалан уколико је n непаран број. Уколико је пак n паран, онда $(n/2) \mid k$. Но, с обзиром да је $k < n$, закључујемо да мора бити $k = n/2$. Није тешко проверити (учините то!) да је у овом случају елемент $\rho^{n/2}$ заиста у центру. Дакле, за парне n је $Z(\mathbb{D}_n) = \{\varepsilon, \rho^{n/2}\}$. ♣

Напомена: Центар групе $\mathbb{D}_n$ могли смо да одредимо и из чињенице да знамо класе конјугације (центар је унија једночланих класа конјугације), али је добро то урадити и директно.

Дефиниција 10 Централизатор елемента $g \in G$, у ознаци, $Z(g)$ је скуп свих елемената групе G који комутирају са g:

$$Z(g) := \{x \in G : xg = gx\}.$$

Став 11 Важи следеће: а) $Z(g) \leq G$;

б) број елемената у класи конјугације елемента $g \in G$ једнак је индексу његовог централизатора.

Доказ. Провера чињенице да је $Z(g)$ подгрупа групе G изводи се на потпуно аналоган начин провери да је $Z(G)$ подгрупа.

Означимо са $C(g)$ класу конјугације елемента g. Другим речима,

$$C(g) = \{gxg^{-1} : g \in G\}.$$

Дефинишемо функцију $f : G/Z(g) \to C(g)$, са

$$f(xZ(g)) = xgx^{-1}.$$

Докажимо да је f добро дефинисана. Дакле, нека је $xZ(g) = yZ(g)$. Треба показати да је $xgx^{-1} = ygy^{-1}$. Но, како је $xZ(g) = yZ(g)$, то је $y^{-1}x \in Z(g)$, па је

$$(y^{-1}x)g = g(y^{-1}x).$$

Множењем ове једнакости слева са y, а здесна са x^{-1} и коришћењем асоцијативности множења добијамо тражени резултат (проверите!).

Јасно је да је f „на“. Докажимо да је f „1–1“. Нека је $f(xZ(g)) = f(yZ(g))$, тј. $xgx^{-1} = ygy^{-1}$. Одавде следи да је $(x^{-1}y)g = g(x^{-1}y)$, тј. $x^{-1}y \in Z(g)$, па је $xZ(g) = yZ(g)$. □

Последица 12 Свака коначна група реда p^n, где је p прост број, а $n \geq 2$, има нетривијалан центар.

Доказ. Као и у случају сваке релације еквиваленције, група G је дисјунктна унија различитих класа конјугације. Осим тога, центар групе G је унија свих једночланих класа конјугације. Добијамо да је

$$G = Z(G) \sqcup C_1 \sqcup \ldots \sqcup C_k, \tag{1}$$

при чему класе C_i нису једночлане. Другим речима,

$$|G| = |Z(G)| + |C_1| + \cdots + |C_k|,$$

при чему је $|C_i| > 1$. Како је $|C_i|$ једнако индексу централизатора (било ког) елемента из C_i и како је $|C_i| \neq 1$, мора бити $p \mid |C_i|$. Из (1) следи да $p \mid |Z(G)|$, па центар заиста није тривијалан. □

Последица 13 Ако је p прост број, онда је свака група реда p^2 или циклична или изоморфна групи $\mathbb{Z}_p \times \mathbb{Z}_p$.

Доказ. Уколико у G постоји елемент реда p^2, група G је циклична. Претпоставимо да у G нема елемената реда p^2. Како према претходном $Z(G)$ није тривијална група, закључујемо да постоји елемент $x \in Z(G)$, који је нужно реда p. Нека је $H = \langle x \rangle$. Уколико је y ма који елемент

из $G \setminus \langle x \rangle$, онда је y такође реда p и нека је $K = \langle y \rangle$. Како је $H \subseteq Z(G)$, сваки елемент из H комутира са сваким из K. Осим тога, ако је $H \cap K \neq \{e\}$, онда је $|H \cap K| = p$, па је $H = H \cap K = K$, што противречи претпоставци. Дакле, $H \cap K = \{e\}$. Уколико још докажемо да је $H \cdot K = G$, према ставу о разлагању на производ, добијамо да је $G \cong H \times K \cong \mathbb{Z}_p \times \mathbb{Z}_p$. Јасно је да је

$$H \cdot K = \{x^r y^s : 0 \leq r < p, 0 \leq s < p\}.$$

Показаћемо да међу овим елементима нема једнаких. Како их има $p^2 = |G|$, одатле добијамо да је $G = H \cdot K$. Претпоставимо да је

$$x^r y^s = x^t y^u.$$

Добијамо да је

$$x^{r-t} = y^{u-s}.$$

Тај елемент је и у H и у K. Како је пресек ових подгрупа тривијалан, закључујемо да је $x^{r-t} = e = y^{u-s}$. Но, како су и r и t ненегативни и мањи од $p = \omega(x)$, закључујемо да је $r - t = 0$, тј. $r = t$. На исти начин добијамо да је $s = v$ те међу наведеним елементима заиста нема једнаких. Дакле, заиста је $G = H \cdot K$, те је доказ завршен. □